

中国

网络密码

第一代

黑客

王凯◎编著

攻伐实录

走进神秘莫测的网络世界 探秘刀光剑影的黑客战场

中国第一代黑客现身说法 传奇的成长经历
曲折的转型过程

揭秘国内外经典黑客事件 中国第一代黑客精彩点评
完全精通黑客攻防全过程

网络密码

中国第一代黑客攻伐实录

王凯◎编著



 电脑报电子音像出版社
CICW ELECTRONIC & AUDIOVISUAL PUBLISHING

内容提要

本手册采用案例的形式,讲述了中国第一代黑客传奇的成长经历和曲折的转型过程,以及他们所亲身经历的黑客事件。循序渐进地介绍了黑客攻击的一般方法、步骤、所使用的工具以及防范的方法、措施。同时还分析了国外一些经典黑客事件中所应用技术的实现和防范全过程。

本手册适用于对计算机安全感兴趣的爱好者以及所有计算机安全领域的技术人员和管理人员。

光盘要目

1. 赠送价值 58 元《eScanAV 麦克沃德》专业级杀毒软件
2. 黑客攻防电子书
3. 黑客攻防视频教程
4. 黑客攻防常用工具
5. 系统杀毒防毒工具

警告: 文中涉及到的黑客攻防相关内容及光盘中提供的工具,仅供读者学习之用,严禁用于任何非法用途,其后果自负。

网络密码

编 著:王 凯

责任编辑:郭 彦

版式设计:郑 兰

出版单位:电脑报电子音像出版社

地 址:重庆市双钢路3号科协大厦

邮政编码:400013

服务电话:(023)63658888-12031

发 行:重庆电脑报经营有限责任公司

经 销:各地新华书店、报刊亭

C D 生产:四川省崑山数码科技文化发展有限公司

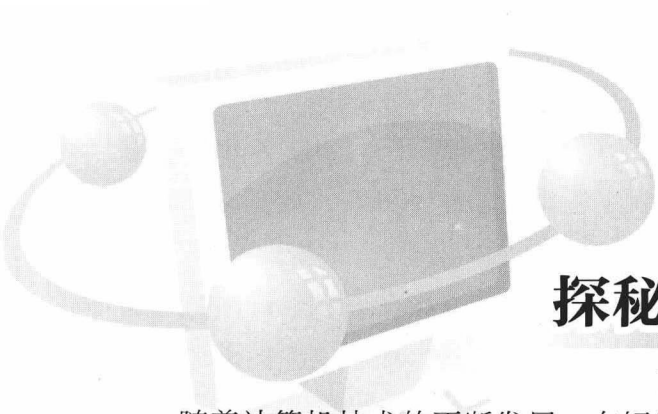
文本印刷:重庆升光电力印务有限公司

开本规格:787mm×1092mm 1/16 16印张 200千字

版 号:ISBN 978-7-89476-624-3

版 次:2011年4月第1版 2011年4月第1次印刷

定 价:39.80元(1CD+手册)



探秘刀光剑影的黑客战场

随着计算机技术的不断发展，在短短的二三十年里，世界就进入了网络信息时代，网络作为一种重要的信息传递手段，对于经济的发展和人们之间的交流起着越来越重要的作用。到了 21 世纪，网络更是已经进入了广大普通市民的日常生活，他们的工作、学习、休闲娱乐都离不开网络。

现在，很多年轻人都成为了名副其实的“网虫”，成天把自己挂在网上，享受着网络世界给他们生活带来的便利和舒适。但是，很多人只知道“网络的世界很精彩”，却忽略了其实“网络的世界也很无奈”。别看我们的电脑屏幕右下角的小狮子欢快的笑着，别看屏幕右下角的盾牌是表示安全的绿色，但此时你在电脑上的一举一动可能都已经在别人的监视之下，而你正欢快地“裸奔”在网络的世界里。

在网络技术蓬勃发展的今天，网络安全问题也受到了日益严峻的考验，甚至到了令人堪忧的地步，一个令人觉得神秘而可怕的名词逐渐进入了我们的世界——黑客。对于绝大多数人来说，黑客是一个非常熟悉却非常陌生的东西，熟悉的是“黑客”这个名词，而陌生的是黑客的真实世界。

黑客的诞生由来已久，就像战争出现于武器的诞生一样，但是在最开始，“黑客”是一种荣耀的名词，它代表着反权威却奉公守法的网络英雄，只是到后来，黑客技术被一些不法分子用来进行恶意破坏或非法牟利之用，黑客的形象开始变得迷离，既可代表英雄又可代表罪犯。

然而要真正了解黑客的性质和对在网络时代中的影响，我们还得通过了解一些黑客的真实事件才行。针对广大黑客迷和计算机网络爱好者们希望深入了解黑客的真实世界这一需要，我们推出了这本黑客攻防实录，希望广大爱好者能从中深刻的了解到黑客的真实世界，了解世界上著名黑客攻击事件的来龙去脉，也可以从中学到不少关于黑客的技术知识。

本实录分为两个部分，共搜集了 13 个实录事件，第一部分介绍了 Coolfire、反黑专家 PP 等中国第一代黑客的传奇经历，第二部分则罗列了大量“蠕虫”病毒等世界上一些著名的黑客病毒和黑客入侵事件，让读者了解这些造成重大影响的事件都是怎么产生的，也许你会惊讶的发现，一个对某个国家或政府机构造成

重大恐慌的黑客竟然就是一个宅在家里因为无聊而“找找乐子”的18岁小伙，或者也可能是一个完全不修边幅，手指甲被烟熏得焦黄的潦倒男人，甚至，可能是一位衣冠楚楚的公司高管。

这就是黑客的世界：他在那头，你在这头；他在暗，你在明。也许你的电脑正遭受黑客的肆意入侵而你却浑然不知，或者即使知道被入侵了也不知道那个人是谁。

所谓“好事不出门，坏事传千里”，世界上著名的黑客事件都是带有一定的恶意入侵行为，所以本书中搜集的一些著名黑客事件基本都是反面的例子，但黑客技术就像枪一样，一把枪既可以帮助好人射击坏人，也可以被坏人用来滥杀好人，就看这把枪握在谁的手里。广大黑客迷们也是一样，你们能从中学到很多实用的黑客知识，但一定不可用来对社会造成混乱，做一个有素质的正面黑客，要做一个真正被人崇拜的黑客，请广大读者在拥有黑客技术的同时还牢记以下几点：

1. 不恶意破坏任何的系统，恶意破坏他人的软体将导致法律责任；
2. 不修改任何的系统，如果你是为了要进入系统而修改它，请在达到目的后将它改回原状；
3. 不要在 bbs 上谈论你 hack 的任何事情；
4. 不要侵入或破坏政府机关的主机；
5. 已侵入电脑中的帐号不得清除或涂改；
6. 不得修改系统档案，如果为了隐藏自己的侵入而做的修改则不在此限，但仍须维持原来系统的安全性，不得因得到系统的控制权而将门户大开。

本实录的定位是初中级读者，内容以实例讲解为主线，从中参入并解读黑客的攻击技术，同时也涵盖了黑客防范、系统加密、安全防范等知识，是了解并掌握黑客初中级技术的实用教程，同时也是了解如何防范恶意黑客的重要参考。

最后编者再次申明：本书的目的是让对黑客感兴趣的读者有一个获取知识的平台，知识无过，善恶在人，请广大读者持正确的心态去阅读和学习，切勿用来进行破坏活动，由此所带来的后果读者自行承担，编者及出版社概不负责！

编者

2011 年 4 月

中国第一代黑客的传奇经历

实录1 开辟鸿蒙的一代宗师Coolfire

人物详解	2
黑客“传道士”	2
黑客守则.....	3
攻击过程还原	3
通过聊天工具查探IP地址	3
通过邮件查看对方IP地址	4
1. E-mail查IP的优点与缺点.....	4
2. 使用Outlook查看邮件发送者IP地址	4
3. Foxmail邮件查IP地址.....	4
锁定攻击目标物理地址.....	5
1. 在线查询IP物理位置	5
2. 使用IP查询专用工具	6

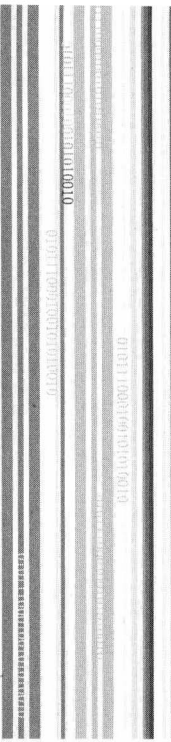
实录2 成功转型的反黑专家PP

人物详解	7
跟着时代步伐前进	7
戴安娜王妃的启迪	7
同在一片天空下.....	8
人生的重要转折点	8

阳光下展开的翅膀	9
攻击过程还原	9
扫描器简介	10
扫描器霸主——X-Scan	10
1. X-Scan简介	10
2. X-Scan界面	10
3. 扫描参数设置	11
4. 扫描模块设置	13
5. 扫描信息	13
最具攻击性的扫描器——“流光”	13
1. 流光简介	13
2. 扫描参数设置	14
3. 开始扫描	15
4. 查看扫描报告	15
强大的端口扫描器——SuperScan	16
1. SuperSan简介	16
2. 获得远程服务器的IP地址	16
3. 扫描某个IP段内的在线主机	17
4. 扫描指定IP主机的端口	17
多功能扫描器——X-Way	18
1. 高级扫描功能	18
2. 主机搜索功能	20
3. 查询功能	21
4. 猜解机	21
5. “黑匣子”攻击	21
6. 嗅探器	22
7. 代理扫描功能	23

实录3 龚蔚与“绿色兵团”

人物详解	24
群英荟萃	24



- 名字由来..... 24
- 穷途末路..... 25
- 攻击过程还原 25**
 - 远程攻击简述..... 25
 - 1.远程攻击简介 25
 - 2.远程攻击分类 26
 - 3.远程攻击的特点 26
 - 远程攻击过程..... 26
 - 1.确定攻击目标 26
 - 2.服务分析 26
 - 3.利用漏洞进行攻击 27
 - DoS拒绝服务攻击..... 27
 - 1.DoS攻击简介 27
 - 2.DoS攻击分类..... 27
 - 3.DoS洪水攻击利器 28
 - 经典远程溢出攻击 30
 - 1. 远程溢出攻击简介 30
 - 2. 扫描远程主机漏洞 31
 - 3. Unicode漏洞攻击..... 33
 - 4. IDA和IDQ扩展溢出漏洞 35
 - 5. Printer溢出漏洞 36
 - 6. WebDAV 缓冲溢出漏洞 37
 - 7. RPC溢出漏洞 38
 - 局域网内的IP攻击 39
 - 1. IP攻击概念及分类 39
 - 2. IP冲突攻击利器——网络特工 39
 - 3. ARP欺骗攻击..... 40
 - 操作系统远程溢出攻击..... 41
 - 1. Wins MS04045溢出攻击..... 41
 - 2. Windows SSL Library远程溢出攻击..... 43
 - 3. Lsasrv. DLL远程溢出攻击..... 44
 - 4. MS04-028 JPEG图片溢出攻击..... 45
 - 5. WindowsXP SP2防火墙溢出攻击..... 46
 - 6. MS05-002漏洞溢出攻击 46

7. IE IFRAME漏洞溢出攻击	47
8. ms05037漏洞远程溢出攻击	47
娱乐软件溢出攻击	50
1. Real Server远程溢出攻击	50
2. Realplay .smil远程溢出攻击	50
3. Windows Media远程溢出漏洞	51

实录4 陈三公子与“第八军团”

人物详解	52
“江湖”扬名	52
“脱黑”之后	52
“公子”其人	52
攻击过程还原	53
WEB攻击简介	53
1. WEB攻击概述及特点	53
2. 常见WEB攻击过程及攻击方式分类	55
SQL注入攻击	57
1. SQL注入攻击基础	57
2. 初级SQL注入攻击与防范	59
3. SQL注入攻击网站数据库	64
4. SQL数据库注入攻击	72
5. PHP注入入侵详解	77
数据库漏洞入侵	80
1. 数据库漏洞入侵简介	80
2. 动网数据库下载漏洞攻击过程	81
3. 通过搜索引擎利用网站数据库入侵	86
文件上传漏洞入侵	87
1. 文件上传漏洞的原理	87
2. 文件上传漏洞利用工具简介	88
3. 文件上传漏洞入侵实例	89

中国第一代黑客眼中的国外著名黑客事件

实录5 让全世界300多家公司电脑系统瘫痪的“梅丽莎”病毒

事件详解	94
“梅丽莎”变种	94
病毒制作者被惩罚	94
攻击过程还原	94
病毒使用技巧	95
1.巧改邮件附件图标	95
2.邮件附件中捆绑木马	96
3.压缩包附件攻击	97
4.图片附件攻击	97
5.文件碎片对象病毒	98
病毒防范技巧	99
1.应用杀毒软件	99
2.恶作剧病毒的清除	105

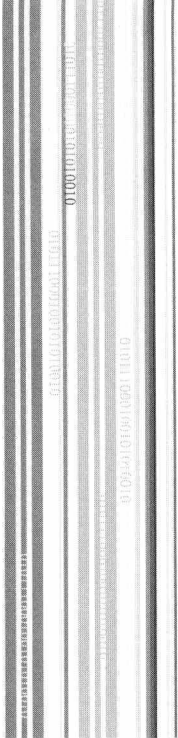
实录6 进入五角大楼翻阅“外星人”资料的加里·麦金农

事件详解	109
入侵美国军方网站	109
入侵事件的影响	110

入侵动机.....	110
受审	111
结局	111
攻击过程还原	111
深入了解木马	112
1. 木马与远程控制	112
2. 木马的分类及攻击方式	114
3. 木马的藏身之处	115
4. 特洛伊木马	117
木马新技术——反弹木马	118
1. 何为反弹式木马	118
2. 反弹式木马的原理	118
3. 反弹木马实例——灰鸽子	118
攻击过程.....	121
1. 配置“黑客之门”	121
2. 用IRC木马进行DDOS攻击.....	124
3. 制作盗号网页木马	127
4. 伪装木马	129

实录7 世界首个“蠕虫”病毒

事件详解	133
蠕虫病毒基本知识	133
1. 防治方法	133
2. 形成原因	133
3. 传播方式	133
蠕虫病毒的特点.....	134
1. 利用程序漏洞	134
2. 病毒制作技术新颖	134
3. 传播手段多样	134
4. 破坏性强	134
攻击过程还原	134



利用IIS错误解码漏洞进行攻击.....134

IIS错误解码漏洞的防范.....135

IIS服务器的安全措施.....136

 1.IIS安全安装.....136

 2.IIS安全配置.....136

实录8 韩国历史上最大的黑客事件

事件详解.....139

攻击过程还原.....139

 旁敲侧击入侵动网论坛.....139

 1.数据库下载入侵动网论坛.....140

 2.巧用大唐美化版插件上传漏洞入侵.....143

 3.美梦破灭，暴破入侵vBulletin3论坛.....144

 入侵BBSXP论坛，巧获WEBSHELL.....146

 1.入侵破解ACCESS版管理员帐号.....146

 2.入侵SQL版BBSXP论坛.....147

 3.上传入侵BBSXP论坛.....148

 4.暴库入侵BBSXP.....149

 PHPwind论坛轻松进.....150

 Discuz! 2.5F论坛恶梦.....151

实录9 号称世界头号黑客的凯文·米特尼克

事件详解.....153

 初露头角.....153

 肆虐网络.....153

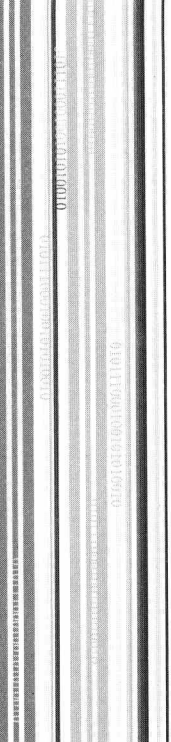
 再次被捕.....154

 起诉与释放.....154

米特尼克对电脑安全的建议	155
攻击过程还原	155
暴力破解必备工具——黑客字典	156
1. 利用“黑客字典II”制作字典文件	156
2. 利用“万能钥匙”制作字典文件	158
加密解密常用工具	158
1. 调试类工具Soft-ICE、Trw2000和后起之秀OllyDbg	158
2. 反汇编工具W32dasm	159
3. 十六进制编辑器Ultraedit、Winhex	159
4. 文件监视工具Filemon	159
5. 侦壳软件PEIDentifier	160
简单的加壳脱壳	160
1. 利用UPXShell、ASPack加壳	160
2. 利用侦壳软件PEIDentifier侦测加壳类型	161
3. 利用UPXShell、AspackDie脱壳	162
破解实例	162
1. 利用“万能可见工具”简单破解“黑客字典II”功能限制	163
2. 爆破“黑客字典II”	163
3. 利用OllyDbg跟踪出“黑客字典II”正确注册码	165
4. 完美破解“黑客字典II”	166

实录10 2009年Pwn20wn全球黑客大赛

事件详解	168
攻击过程还原	168
IE执行任意程序攻击	168
1. Web聊天室执行任意程序攻击	168
2. 利用chm文件执行任意程序攻击	169
3. 利用IE执行本地可执行文件攻击	171
IE炸弹攻击与防范	173
1. IE炸弹的攻击类型	173
2. IE窗口炸弹的防御	174



IE处理异常MIME漏洞 174

 1.利用MIME漏洞进行木马攻击 175

 2.利用MIME漏洞恶意代码攻击 176

 3.防范利用MIME漏洞的攻击 178

恶意网页修改系统 179

 1.网页恶意代码剖析 180

 2.利用Office对象删除硬盘文件..... 181

 3.利用Office宏删除硬盘文件..... 183

 4.利用ActiveX对象删除硬盘文件..... 184

 5.利用网页实施攻击 186

 6.万花谷病毒实施攻击 187

 7.将访问者的硬盘设为共享 190

浏览器安全防范..... 191

 1.防范网页恶意代码 191

 2.网页泄密及防范 193

 3.网址泄密及防范 194

 4.Cookie泄密及防范 195

 5.使用O E查看邮件信息漏洞 196

实录11 黑客入侵纳斯达克事件

事件详解 198

攻击过程还原 198

 WEB浏览的安全防护 198

 1.程序下载的安全隐患 198

 2.选择性安装插件 198

 3.禁用Cookie 199

 4.删除IE历史记录 199

 5.升级IE浏览器 200

 防范网页“黑手” 200

 1.如何防止硬盘被格式化 201

 2.如何防止系统资源耗尽 201

 3.如何防止控制权限被窃取 201

预防网络攻击	201
1. 设定安全级别	201
2. 过滤指定网页	202
3. 卸载或升级WSH	202
4. 禁用远程注册表服务	202
网络安全防御基本方法	203
1. 禁用没用的服务	203
2. 安装补丁程序	203
安全使用邮件	203
1. 把垃圾邮件放到垃圾邮件文件夹里	204
2. 遇到攻击时向自己所在的ISP求援	204
3. 不随意公开自己的信箱地址	204
4. 采用过滤功能	205
5. 隐藏自己的电子邮件地址	205
6. 谨慎使用自动回信功能	205
7. 使用转信功能	206
8. 保护邮件列表中的E-mail地址	206
9. 时刻警惕邮件病毒的袭击	206
10. 拒绝“饼干”信息	206
11. 邮件远程管理	207
使用Ghost备份数据	207
1. 系统备份	207
2. 系统恢复	208

实录12 Google视频播放器破解事件

事件详解	210
攻击过程还原	210
突破网页锁定鼠标右键	210
1. 突破方法一	210
2. 突破方法二	211
3. 突破方法三	212

使用Office XP编辑网页	213
1. 编辑方法一	213
2. 编辑方法二	213
对页面垃圾说再见	214
巧除免费主页空间的广告条	215
1. CHINADNS.COM的弹出广告去除办法	215
2. 51.net去广告的办法	215
3. www.yeskey.net的去广告转向域名	215
使用NTFS权限拒收QQ广告	215
让电脑自动填写网页注册信息	216
让电脑自动进行网站注册	217
让ICQ发送超长字符的消息	218
如何在论坛帖中加入表情符	218
自己定制IE的外观	218
增强IE对网址的自动识别能力	218
去掉IE全屏显示时的工具栏	219
定制IE的高级选项	220
删除IE页面中链接的下划线	220
IE显示超级链接的完整地址	221
保持远程连接	221
通过Web方式使用打印机	222
恢复被修改的IE默认主页	222
使用IE的黑名单功能阻止广告	222
修改IE默认主页	223
广告克星AdFilter	223
1. Main (主选项)	224
2. Update (软件更新)	224
3. Statitics (统计信息)	224
4. Exceptions (排除过滤设置)	224
5. Setup (其他设置)	225

IE插件全攻略	225
1. Microgarden WebTools	225
2. Flash Catcher	225
3. IE文件下载增强插件	225

实录13 黑客与电力系统

事件详解	226
攻击过程还原	226
开机加密	227
Windows登录加密	227
1. Windows 2000登录加密	227
2. Windows XP登录加密	229
文件与文件夹加密	230
1. 利用文件夹属性进行简单加密	230
2. 利用软件自带的加密功能加密	231
利用文件压缩加密	232
1. WinZip文件加密	232
2. WinRAR文件加密	233
隐藏驱动器	233
应用万能加密器加密	235
1. 文件加密	235
2. 文件解密	236
编译EXE文件	236
分割文件	237
文件嵌入	238
伪装目录	239